STACK Cybersecurity Cyber Readiness Checklist

Use this checklist to assess your company's cyber resilience posture

Identity & Access Controls

- □ Phishing-resistant multi-factor authentication (MFA) deployed across all critical systems
- □ Inventory of privileged accounts with just-in-time access enabled
- □ Continuous identity validation (behavior-based monitoring)
- □ Credential rotation schedule established
- □ Passwordless authentication roadmap in development

Threat Detection & Response

- □ EDR deployed on every endpoint
- □ 24/7 monitoring with AI-assisted detection
- □ Incident response playbooks tested quarterly
- □ MTTD/MTTR tracked and reported to leadership
- □ Automated security orchestration implemented

Resilience & Continuity

- □ Backup integrity and restoration tested monthly
- □ Downtime cost modeling completed for core services
- □ Tabletop exercises covering ransomware scenarios conducted
- □ Supply chain disruption scenarios included in exercises
- □ Business continuity plans updated within last 6 months

STACK CYBERSECURITY

Vendor & Supply Chain Risk

- □ Vendor cyber attestation program in place
- □ Critical vendors mapped to business impact
- □ Real-time scoring or continuous monitoring tools deployed
- □ Third-party risk assessments conducted annually
- □ Contract language includes cybersecurity requirements

Cloud & Application Security

- □ Misconfiguration scanning implemented
- □ CNAPP (Cloud-Native Application Protection Platform) coverage
- □ API security validation processes established
- □ Zero-trust segmentation across cloud workloads
- □ Cloud security posture management tools deployed

Compliance & Governance

- □ Real-time compliance dashboards for relevant frameworks (DORA, NIS2, HIPAA, PCI, etc.)
- □ Audit-ready logging and documentation maintained
- □ Annual risk quantification tied to financial outcomes
- □ Board receives regular cyber resilience reports
- □ Cyber metrics included in executive scorecards

STACK CYBERSECURITY

Quantum & Future Risk Readiness

- □ Encryption asset inventory completed
- □ Post-quantum cryptography roadmap established
- □ Long-term data retention and decryption risks assessed
- □ Cryptographic agility programs initiated
- □ Quantum-resistant algorithms evaluation in progress

Assessment

If your company is missing more than a quarter of these controls, your resilience posture is not aligned with current threat economics.

Next Steps

1. Score your organization (count completed items)
2. Identify your top 5 gaps based on business risk
3. Prioritize investments
4. Set quarterly targets for improvement
5. Assess every 6 months